日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１２月１８日

出願番号
Application Number: 特願２００２－３６６２４３

[ST.10/C]: ［ＪＰ２００２－３６６２４３］

出願人
Applicant(s): 株式会社山武

２００３年　７月　４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５３４６７

【書類名】　特許願
【整理番号】　20020317
【提出日】　平成14年12月18日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
　【氏名】　三島　崇
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
　【氏名】　佐内　大司
【特許出願人】
　【識別番号】　000006666
　【氏名又は名称】　株式会社　山武
【代理人】
　【識別番号】　100095072
　【弁理士】
　【氏名又は名称】　岡田　光由
　【電話番号】　03-3807-1818
【手数料の表示】
　【予納台帳番号】　012944
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9722522

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　パスワード作成支援方法及びパスワード作成支援プログラム

【特許請求の範囲】

【請求項１】　作成支援対象のパスワードと、そのパスワードに含まれる検査対象の文字列を特定するための文字位置の情報とを入力する過程と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、上記文字位置に上記文字列を持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する過程と、

上記取得したパスワード候補の生成個数に従って、上記文字列の強度を算出する過程と、

上記算出した文字列強度の情報を出力する過程とを備えることを、

特徴とするパスワード作成支援方法。

【請求項２】　作成支援対象のパスワードを入力する過程と、

上記入力したパスワードを構成する全ての文字あるいは一部の文字を、その文字位置とともに抽出する過程と、

上記抽出した文字及び文字位置をキーにして、パスワード推測ツールに備えられて、パスワードの推測を総当たりで行う際に用いられる各文字位置毎の文字順序の情報を記録するテーブル群を参照することで、上記抽出した文字のそれぞれについて、上記抽出した文字位置における文字順序を特定する過程と、

上記特定した文字順序に従って、上記抽出した文字のそれぞれについて文字強度を算出する過程と、

上記算出した文字強度の情報を出力する過程とを備えることを、

特徴とするパスワード作成支援方法。

【請求項３】　作成支援対象のパスワードを入力する過程と、

上記入力したパスワードの先頭の文字を開始文字として、１文字ずつ長さの長くなる文字列を抽出する過程と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパ

スワード候補を生成するパスワード候補ツールを使って、上記抽出した文字列のそれぞれについて、それらの文字列を同じ文字位置に持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する過程と、

上記取得したパスワード候補の生成個数に従って、上記入力したパスワードの文字強度の推移値を算出する過程と、

上記算出した文字強度推移値を出力する過程とを備えることを、

特徴とするパスワード作成支援方法。

【請求項４】　作成支援対象のパスワードと、そのパスワードに含まれる検査対象の文字列を特定するための文字位置の情報とを入力する処理と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、上記文字位置に上記文字列を持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する処理と、

上記取得したパスワード候補の生成個数に従って、上記文字列の強度を算出する処理と、

上記算出した文字列強度の情報を出力する処理とをコンピュータに実行させるためのパスワード作成支援プログラム。

【請求項５】　作成支援対象のパスワードを入力する処理と、

上記入力したパスワードを構成する全ての文字あるいは一部の文字を、その文字位置とともに抽出する処理と、

上記抽出した文字及び文字位置をキーにして、パスワード推測ツールに備えられて、パスワードの推測を総当たりで行う際に用いられる各文字位置毎の文字順序の情報を記録するテーブル群を参照することで、上記抽出した文字のそれぞれについて、上記抽出した文字位置における文字順序を特定する処理と、

上記特定した文字順序に従って、上記抽出した文字のそれぞれについて文字強度を算出する処理と、

上記算出した文字強度の情報を出力する処理とをコンピュータに実行させるためのパスワード作成支援プログラム。

【請求項６】　作成支援対象のパスワードを入力する処理と、

上記入力したパスワードの先頭の文字を開始文字として、１文字ずつ長さの長くなる文字列を抽出する処理と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補ツールを使って、上記抽出した文字列のそれぞれについて、それらの文字列を同じ文字位置に持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する処理と、

上記取得したパスワード候補の生成個数に従って、上記入力したパスワードの文字強度の推移値を算出する処理と、

上記算出した文字強度推移値を出力する処理とをコンピュータに実行させるためのパスワード作成支援プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パスワードの作成を支援するパスワード作成支援方法と、そのパスワード作成支援方法の実現に用いられるパスワード作成支援プログラムとに関し、特に、パスワードのどの部分が強くどの部分が弱いのかを分析して出力することで、強いパスワードの作成を支援するパスワード作成支援方法と、そのパスワード作成支援方法の実現に用いられるパスワード作成支援プログラムとに関する。

【０００２】

【従来の技術】

ユーザがコンピュータ上で動作するシステムを利用する場合には、ユーザに対して、予めコンピュータに登録させたパスワードと同一のパスワードを入力させるようにすることで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００３】

コンピュータに登録されるパスワードは、盗まれる可能性があることから暗号化されており、これから、システムの利用時にユーザから平文のパスワードが入力されると、それを暗号化して、この登録されている暗号化パスワードと一致す

るのか否かを判断することで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００４】

ところで、セキュリティを確保するためには、強いパスワードを付けることが必須である。しかしながら、現在、どのようなパスワードを使えば強いと言えるのか明確な指標はない。

【０００５】

これから、ユーザは、どのようなパスワードを付ければよいのかよく分からないというのが実情である。「長いパスワードを使う」とか、「英数字記号を混ぜる」などのアドバイスがあるものの、実際に、どのようなパスワードを付ければよいのかよく分からないというのが実情である。

【０００６】

【発明が解決しようとする課題】

このようなことを背景にして、本発明者らは、先に出願した特願２００２－２９８１９０で、数値的に表現されるパスワードの強度を実用的な時間内に算出できるようにする新たなパスワード強度検査技術を提案した。

【０００７】

この特願２００２－２９８１９０で開示した発明では、パスワードに対するブルートフォース攻撃に耐えられる時間の長さを測定することで、パスワードの強度を得るようにしている。

【０００８】

ブルートフォース攻撃では、図１４に示すように、パスワードとして使用できるすべての文字を組み合わせることで平文のパスワード候補を生成して、それを暗号化したものがコンピュータに登録されている暗号化パスワードと一致するのか否かについて判断することを繰り返していくことで、その暗号化パスワードに対応付けられる平文のパスワードを盗み取るようにしている。

【０００９】

このブルートフォース攻撃に用いられるパスワード推測ツールとして、最近では、効率的なブルートフォース攻撃を行うために、文字の出現頻度の統計情報に

基づいてパスワード候補を生成する「Ｊohn the Ｒipper 」のようなパスワード推測ツールが用いられている（三島など:"ブルートフォースに勝つ“強いパスワード”とは",日経ネットワークセキュリティ,Vol.2,pp.36-47(2002)）。

【００１０】

特願２００２－２９８１９０で開示した発明では、このような文字の出現頻度の統計情報に基づいてパスワード候補を生成する「Ｊohn the Ｒipper 」などのようなパスワード推測ツールを想定して、検査対象のパスワードがそのパスワード推測ツールの何番目に生成されるのか（ブルートフォース攻撃に耐えられる時間の長さに対応付けられる）を特定することで、検査対象のパスワードの強度を測定するようにしている。

【００１１】

この測定にあたって、特願２００２－２９８１９０で開示した発明では、検査対象のパスワードの強度測定を実用的な時間内に実現するために、パスワード推測ツールの生成した暗号化前のパスワード候補と検査対象の平文のパスワードとを照合することで、検査対象のパスワードの強度を測定するようにしている。

【００１２】

確かに、特願２００２－２９８１９０で開示した発明によれば、数値的に表現されるパスワードの強度を実用的な時間内に算出できるようになる。

【００１３】

しかしながら、特願２００２－２９８１９０で開示した発明では、パスワード全体としての強さを数値的に把握することができるようになるものの、パスワードのどの部分が強くどの部分が弱いのかについては把握することができず、改善の余地が残されている。

【００１４】

本発明はかかる事情に鑑みてなされたものであって、パスワードのどの部分が強くどの部分が弱いのかを分析して出力することで、強いパスワードの作成を支援する新たなパスワード作成支援技術の提供を目的とする。

【００１５】

【課題を解決するための手段】

（１）第１の構成

この目的を達成するために、本発明は、①作成支援対象のパスワードと、そのパスワードに含まれる検査対象の文字列を特定するための文字位置の情報とを入力する過程と、②パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、その文字位置に検査対象の文字列を持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する過程と、③取得したパスワード候補の生成個数に従って、検査対象の文字列の強度を算出する過程と、④算出した文字列強度の情報を出力する過程とを備えるように構成する。

【００１６】

以上の各処理過程はコンピュータプログラムで実現できるものであり、このコンピュータプログラムは、半導体メモリなどの記録媒体に記録して提供したり、ネットワークを介して提供することができる。

【００１７】

このように構成される本発明では、例えば「ｔａｎａｋａ」という作成支援対象のパスワードと、例えば先頭から３文字及び５文字という文字位置の情報とを入力することで、検査対象となる「ｎａｋ」という文字列を入力すると、パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、その文字位置に「ｎａｋ」という文字列を持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する。

【００１８】

続いて、その取得したパスワード候補の生成個数に従って、検査対象の文字列の強度を算出して、それを出力する。

【００１９】

このようにして、本発明によれば、パスワードに含まれる文字列について、その強度が出力されることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【００２０】

（２）第２の構成

この目的を達成するために、本発明は、①作成支援対象のパスワードを入力する過程と、②入力したパスワードを構成する全ての文字あるいは一部の文字を、その文字位置とともに抽出する過程と、③抽出した文字及び文字位置をキーにして、パスワード推測ツールに備えられて、パスワードの推測を総当たりで行う際に用いられる各文字位置毎の文字順序の情報を記録するテーブル群を参照することで、抽出した文字のそれぞれについて、抽出した文字位置における文字順序を特定する過程と、④特定した文字順序に従って、抽出した文字のそれぞれについて文字強度を算出する過程と、⑤算出した文字強度の情報を出力する過程とを備えるように構成する。

【００２１】

以上の各処理過程はコンピュータプログラムで実現できるものであり、このコンピュータプログラムは、半導体メモリなどの記録媒体に記録して提供したり、ネットワークを介して提供することができる。

【００２２】

このように構成される本発明では、例えば「ｔａｎａｋａ」という作成支援対象のパスワードを入力すると、第１文字目が「ｔ」で、第２文字目が「ａ」で、第３文字目が「ｎ」で、第４文字目が「ａ」で、第５文字目が「ｋ」で、第６文字目が「ａ」であるということを抽出する。

【００２３】

続いて、パスワード推測ツールに備えられて、パスワードの推測を総当たりで行う際に用いられる各文字位置毎の文字順序の情報を記録するテーブル群を参照することで、例えば９５文字の内の１０番目に出現するというように、第１文字目における「ｔ」の出現する順序、第２文字目における「ａ」の出現する順序、第３文字目における「ｎ」の出現する順序、第４文字目における「ａ」の出現する順序、第５文字目における「ｋ」の出現する順序、第６文字目における「ａ」の出現する順序を特定する。

【００２４】

続いて、その特定した文字順序に従って、抽出した文字のそれぞれについて文字強度を算出して、それを出力する。

【００２５】

このようにして、本発明によれば、パスワードの持つ各文字毎に、その強度が出力されることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【００２６】

（３）第３の構成

この目的を達成するために、本発明は、①作成支援対象のパスワードを入力する過程と、②入力したパスワードの先頭の文字を開始文字として、１文字ずつ長さの長くなる文字列を抽出する過程と、③パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補ツールを使って、抽出した文字列のそれぞれについて、それらの文字列を同じ文字位置に持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する過程と、④取得したパスワード候補の生成個数に従って、入力したパスワードの文字強度の推移値を算出する過程と、⑤算出した文字強度推移値を出力する過程とを備えるように構成する。

【００２７】

以上の各処理過程はコンピュータプログラムで実現できるものであり、このコンピュータプログラムは、半導体メモリなどの記録媒体に記録して提供したり、ネットワークを介して提供することができる。

【００２８】

このように構成される本発明では、例えば「ｔａｎａｋａ」という作成支援対象のパスワードを入力すると、「ｔ」という文字列、「ｔａ」という文字列、「ｔａｎ」という文字列、「ｔａｎａ」という文字列、「ｔａｎａｋ」という文字列、「ｔａｎａｋａ」という文字列を抽出する。

【００２９】

続いて、これらの抽出した文字列のそれぞれについて、パスワード推測ツール

で用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、例えば「ｔａｎａ」という文字列を同じ文字位置に持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数というように、それらの文字列を同じ文字位置に持つパスワード候補が最初に生成されるまでのパスワード候補の生成個数を取得する。

【００３０】

続いて、その取得したパスワード候補の生成個数に従って、入力したパスワードの文字強度の推移値を算出して、それを出力する。

【００３１】

このようにして、本発明によれば、パスワードの持つ文字の文字強度の推移値が出力されることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【００３２】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【００３３】

図１に、本発明を具備するパスワード作成支援装置１の一実施形態例を図示する。

【００３４】

この図に示す本発明を具備するパスワード作成支援装置１は、パスワードの作成を支援する処理を行うものであって、ユーザとの対話手段となる入出力装置１０と、「Ｊohn the Ｒipper」などのようなパスワード推測ツールで用いられて、平文のパスワード候補を生成するパスワード候補生成ルーチン１１と、パスワード候補生成ルーチン１１を使って、検査対象のパスワードの持つ文字列についての強度を算出する文字列強度算出プログラム１２と、パスワード候補生成ルーチン１１の備えるブルートフォース用文字テーブル１５を参照することで、検査対象のパスワードの持つ各文字毎の強度を算出する文字強度算出プログラム１３と、パスワード候補生成ルーチン１１を使って、検査対象のパスワードの持つ文

字の文字強度の推移値を算出する文字強度推移値算出プログラム１４とを備える。

【００３５】

ここで、本発明を実現すべく用意される文字列強度算出プログラム１２や文字強度算出プログラム１３や文字強度推移値算出プログラム１４は、半導体メモリなどの記録媒体に記録して提供されたり、ネットワークを介して提供されることになる。

【００３６】

パスワード候補生成ルーチン１１は、「Ｊohn the Ｒipper」などのようなパスワード推測ツールで用いられて、例えば、最初は、辞書に記載された文字列を使って平文のパスワード候補を生成し、続いて、パスワードとして使用できるすべての文字列を使って平文のパスワード候補を生成していくことで、７兆を超える平文のパスワード候補を規定の順番に従って生成するように処理する。

【００３７】

このパスワード候補の生成にあたって、パスワード候補生成ルーチン１１は、ブルートフォース用文字テーブル１５を使用する。

【００３８】

図２に、ブルートフォース用文字テーブル１５のテーブル構造の一例を図示する。ここで、この図に示すブルートフォース用文字テーブル１５は、「Ｊohn the Ｒipper」のパスワード推測ツールが備えるものを想定している。

【００３９】

「Ｊohn the Ｒipper」のパスワード推測ツールでは、９５個の文字（数字や記号を含む）を使って８桁のパスワード候補を順次生成することでパスワードの推測を行うことになるが、そのパスワード候補の生成にあたって、各桁（各文字位置）毎に、統計情報に従って、どういう文字の順番（その桁での出現頻度の大きい文字の順番）にパスワード候補を生成するのかについて規定している。

【００４０】

この文字の順番を管理するものが図２に示すブルートフォース用文字テーブル１５であって、各桁に対応付けて設けられる文字順序テーブルを使って、各桁毎

に、統計情報に従って、どういう文字の順番にパスワード候補を生成するのかについて規定している。

【００４１】

ここで、「Ｊohn the Ｒipper」のパスワード推測ツールの場合には、図２に示すように、１つ前の桁の文字がｎで、それより更に１つ前の桁の文字がａである場合には、この桁ではこの文字順序テーブルを使うというように、１つ前の桁の文字と、それより更に１つ前の桁の文字とに応じて、その桁で使用する文字順序テーブルが決定されることになっている。

【００４２】

次に、図３に示す処理フローに従って、本発明を実現するために文字列強度算出プログラム１２が実行する処理について説明する。

【００４３】

文字列強度算出プログラム１２は、入出力装置１０のディスプレイに、図４に示すような検査対象のパスワードの入力域と文字開始位置（ｘ桁）／文字終了位置（ｙ桁）の入力域とを持つパスワード強度検査画面を表示しているときに、ユーザから、それらの入力域に対して、検査対象のパスワードと文字列の切り出し位置となるｘ桁／ｙ桁とを入力してパスワード強度の検査要求が発行されると、図３の処理フローに示すように、先ず最初に、ステップ１０で、検査対象のパスワードと文字列の切り出し位置となるｘ桁／ｙ桁とを入力する。

【００４４】

続いて、ステップ１１で、入力したパスワードから、入力したｘ桁／ｙ桁の指す文字列を抽出する。例えば、図５に示すように、パスワード強度検査画面に、「ｔａｎａｋａ」という検査対象のパスワードと「ｘ＝３，ｙ＝５」とが入力される場合には、入力したｘ桁／ｙ桁の指す文字列である「ｎａｋ」を抽出するのである。

【００４５】

続いて、ステップ１２で、パスワード候補の生成個数を示す変数ｊに１をセットし、続くステップ１３で、パスワード候補生成ルーチン１１に対して、パスワード候補の生成を指示する。

【００４６】

このパスワード候補の生成指示を受け取ると、パスワード候補生成ルーチン１１は、パスワード推測ツールで用いられるときと同様の手順に従って、今回初めてパスワード候補を生成するときには、最初のパスワード候補（平文）を生成し、前回パスワード候補を生成しているときには、前回生成したパスワード候補に続くパスワード候補（平文）を１つ生成する。

【００４７】

これから、続いて、ステップ１４で、パスワード候補生成ルーチン１１から、その生成されたパスワード候補を受け取り、続くステップ１５で、その受け取ったパスワード候補から、入力したｘ桁／ｙ桁の指す文字列を抽出する。

【００４８】

続いて、ステップ１６で、ステップ１１で抽出した文字列とステップ１５で抽出した文字列とが一致するのか否かを判断して、一致しないことを判断するときには、ステップ１７に進んで、変数ｊの値を１つインクリメントしてから、次のパスワード候補の生成を指示すべくステップ１３に戻る。

【００４９】

一方、ステップ１６で、ステップ１１で抽出した文字列とステップ１５で抽出した文字列とが一致することを判断するときには、ステップ１８に進んで、ｊの値から、入力パスワードの持つ入力したｘ桁／ｙ桁の指す文字列の強度を算出する。

【００５０】

例えば、ｊの値（これまでに受け取ったパスワード候補の個数）と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数との比率値ｔ（０≦ｔ≦１）

$$t = j / (\text{パスワード候補最大生成可能個数})$$

を算出して、

$$\text{得点} = 100 \times t$$

という算出式に従って、入力したパスワードの強度を示す得点を算出するのである。

【００５１】

そして、最後に、ステップ１９で、図５に示すように、その算出したパスワード強度をパスワード強度検査画面に出力して、処理を終了する。

【００５２】

このようにして、文字列強度算出プログラム１２は、検査対象のパスワードに含まれる指定される文字列について、その強度を算出して出力するように処理するのである。

【００５３】

これにより、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになることで、強いパスワードを作成することができるようになる。

【００５４】

ここで、図３の処理フローでは、検査対象のパスワードに含まれる１つの文字列についてその強度を算出するようにしているが、検査対象のパスワードに含まれる複数の文字列を処理対象として、それらの文字列の強度を算出するようにしてもよい。

【００５５】

次に、図６に示す処理フローに従って、本発明を実現するために文字強度算出プログラム１３が実行する処理について説明する。

【００５６】

文字強度算出プログラム１３は、ユーザから、検査対象のパスワードを指定してパスワード強度の検査要求が発行されると、図６の処理フローに示すように、先ず最初に、ステップ２０で、検査対象のパスワードを入力し、続くステップ２１で、入力したパスワードの文字位置（桁位置）を示す変数ｉに先頭の文字位置を示す１をセットする。

【００５７】

続いて、ステップ２２で、入力したパスワードの先頭の文字から数えて第ｉ－２番目の文字、第ｉ－１番目の文字、第ｉ番目の文字を抽出する。ここで、第ｉ－２番目の文字や第ｉ－１番目の文字の文字が存在しない場合（ｉ＝１，２の場

合）には、存在する文字まで抽出することになる。

【００５８】

続いて、ステップ２３で、抽出した文字をキーにして図２に示すようなデータ構造を持つブルートフォース用文字テーブル１５を辿ることで、第ｉ番目の文字についての文字順序テーブルを特定する。

【００５９】

図２に示すブルートフォース用文字テーブル１５では、１つ前の桁の文字と、それより更に１つ前の桁の文字とに応じて、その桁で使用される文字順序テーブルが特定されることになるので、ステップ２２で抽出した３つの文字をキーにしてブルートフォース用文字テーブル１５を辿ることで、第ｉ番目の文字についての文字順序テーブルを特定するのである。

【００６０】

続いて、ステップ２４で、特定した文字順序テーブルに登録される第ｉ番目の文字の登録位置を検索する。

【００６１】

図２で説明したように、各文字順序テーブルには、パスワードを構成する例えは９５個のそれぞれの文字について、その文字位置で出現する頻度の大きい順に文字が登録されているので、その登録位置を検索するのである。

【００６２】

続いて、ステップ２５で、検索した登録位置に従って、入力したパスワードの第ｉ番目の文字の強度を算出する。

【００６３】

すなわち、文字順序テーブルの登録位置が先頭に近い（値が小さい）ほど出現頻度が大きいことでブルートフォース攻撃に弱い文字であることを示しているので、例えば、検索した登録位置と文字順序テーブルに登録される文字数（例えば９５個）との比率値を算出し、それを０～１００の範囲に規格化することで、入力したパスワードの第ｉ番目の文字の強度を算出するのである。

【００６４】

続いて、ステップ２６で、変数ｉの値を１つインクリメントし、続くステップ

２７で、変数ｉの値がｉmax(入力したパスワードの文字数）よりも大きくなったのか否かを判断して、大きくなっていないことを判断するときには、次の文字位置の文字について処理を行うべくステップ２２に戻り、大きくなったことを判断するときには、ステップ２８に進んで、図７に示すように、算出した文字強度を入出力装置１０のディスプレイに出力して、処理を終了する。

【００６５】

このようにして、文字強度算出プログラム１３は、検査対象のパスワードの持つ各文字毎に、その強度を算出して出力するように処理するのである。

【００６６】

これにより、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになることで、強いパスワードを作成することができるようになる。

【００６７】

ここで、図６の処理フローでは、検査対象のパスワードの持つ全ての文字についてその強度を算出するようにしているが、検査対象のパスワードの持つ一部の文字についてその強度を算出するようにしてもよい。

【００６８】

次に、図８及び図９に示す処理フローに従って、本発明を実現するために文字強度推移値算出プログラム１４が実行する処理について説明する。

【００６９】

文字強度推移値算出プログラム１４は、ユーザから、検査対象のパスワードを指定してパスワード強度の検査要求が発行されると、図８及び図９の処理フローに示すように、先ず最初に、ステップ３０で、検査対象のパスワードを入力する。

【００７０】

続いて、ステップ３１で、入力したパスワードの文字位置（桁位置）を示す変数ｉに先頭の文字位置を示す１をセットし、続くステップ３２で、入力したパスワードの第１番目の文字（先頭の文字）から第ｉ番目の文字までの文字列を抽出する。

【００７１】

続いて、ステップ３３で、パスワード候補の生成個数を示す変数ｊに１をセットし、続くステップ３４で、パスワード候補生成ルーチン１１に対して、パスワード候補の生成を指示する。

【００７２】

このパスワード候補の生成指示を受け取ると、パスワード候補生成ルーチン１１は、パスワード推測ツールで用いられるときと同様の手順に従って、今回初めてパスワード候補を生成するときには、最初のパスワード候補（平文）を生成し、前回パスワード候補を生成しているときには、前回生成したパスワード候補に続くパスワード候補（平文）を１つ生成する。

【００７３】

これから、続いて、ステップ３５で、パスワード候補生成ルーチン１１から、その生成されたパスワード候補を受け取り、続くステップ３６で、その受け取ったパスワード候補の第１番目の文字（先頭の文字）から第ｉ番目の文字までの文字列を抽出する。

【００７４】

続いて、ステップ３７で、ステップ３２で抽出した文字列とステップ３６で抽出した文字列とが一致するのか否かを判断して、一致しないことを判断するときには、ステップ３８に進んで、変数ｊの値を１つインクリメントしてから、次のパスワード候補の生成を指示すべくステップ３４に戻る。

【００７５】

一方、ステップ３７で、ステップ３２で抽出した文字列とステップ３６で抽出した文字列とが一致することを判断するときには、ステップ３９に進んで、ｊの値から、入力したパスワードの第ｉ番目の文字の文字強度推移値を算出する。

【００７６】

例えば、ｊの値（これまでに受け取ったパスワード候補の個数）と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数との比率値ｔ（０≦ｔ≦１）

ｔ＝ｊ／（パスワード候補最大生成可能個数）

を算出して、

得点＝１００×ｔ

という算出式に従って、入力したパスワードの強度を示す得点を算出するのである。

【００７７】

続いて、ステップ４０で、変数ｉの値を１つインクリメントし、続くステップ４１で、変数ｉの値がｉmax(入力したパスワードの文字数）よりも大きくなったのか否かを判断して、大きくなっていないことを判断するときには、次の文字位置の文字について処理を行うべくステップ３２に戻り、大きくなったことを判断するときには、ステップ４２に進んで、図１０に示すように、算出した文字強度推移値を入出力装置１０のディスプレイに出力して、処理を終了する。

【００７８】

このようにして、文字強度推移値算出プログラム１４は、検査対象のパスワードの持つ文字の文字強度の推移値を算出して出力するように処理するのである。

【００７９】

これにより、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになることで、強いパスワードを作成することができるようになる。

【００８０】

ここで、「得点＝１００×ｔ」のような形で求まる文字強度の推移値をそのまま出力するのではなくて、図１１に示すように、文字強度の推移値が小さい所では実際の値よりも大きな値になるようにと変換を行って、それを出力するようにしてもよい。

【００８１】

これは、人の作成するパスワードは一般的に弱いものが多く、図１１に示すような変換を行わずに出力してしまうと、文字強度の推移値の変化がよく分からないことが起こるからである。

【００８２】

また、図８及び図９の処理フローでは、検査対象のパスワードの持つ全ての文

字を処理対象として文字強度の推移値を算出するようにしているが、検査対象のパスワードの持つ一部の文字を処理対象として文字強度の推移値を算出するようにしてもよい。

【００８３】

また、図８及び図９の処理フローでは、説明を簡単にするために、入力したパスワードの第１番目の文字から第ｉ番目の文字までの文字列についての処理を終了すると、第１番目の文字から第ｉ＋１番目の文字までの文字列についてパスワード候補の生成を最初からやり直していくことで説明したが、そのような方法を用いずに、第１番目の文字から第ｉ番目の文字までの文字列についての処理に続けてパスワード候補を生成するようにしてもよいことは言うまでもない。

【００８４】

図８及び図９の処理フローから分かるように、文字強度推移値算出プログラム１４が算出する文字強度推移値は、単純に、パスワードの持つ各文字の文字強度を示している訳ではなくて、先頭からの文字の並びに応じた各文字の文字強度を示している。

【００８５】

これから、図１２に示すように、文字強度算出プログラム１３の算出する文字毎の強度と、文字強度推移値算出プログラム１４の算出する文字強度の推移値とを同じパスワード強度検査画面に出力するようにすると、ユーザは、パスワードのどの部分が強くどの部分が弱いのかについて、より正確に把握できるようになる。

【００８６】

例えば、図１２に示すパスワードでは最後の文字が“ａ”となっている。この文字“ａ”は、文字強度算出プログラム１３の算出する文字強度で見れば分かるように、最後の文字としてよく使われる文字であるものの、文字強度推移値算出プログラム１４の算出する文字強度推移値で見れば分かるように、「ｔ＠＠ｎ（Ｋａ」と並ぶ文字列のパスワードの強度を高めるように作用している。

【００８７】

これに対して、この文字“ａ”の代わりに“＝”という文字を使用する場合に

は、図１３に示すように、この文字“＝”は、文字強度算出プログラム１３の算出する文字強度で見れば分かるように、最後の文字としてあまり使われない文字にもかかわらず、文字強度推移値算出プログラム１４の算出する文字強度推移値で見れば分かるように、「ｔ＠＠ｎ（Ｋ＝」と並ぶ文字列のパスワードの強度をほとんど高めてはいない。

【００８８】

このように、文字強度算出プログラム１３の算出する文字毎の強度と、文字強度推移値算出プログラム１４の算出する文字強度の推移値とを同じパスワード強度検査画面に出力するようにすると、ユーザは、パスワードのどの部分が強くどの部分が弱いのかについて、より正確に把握できるようになるのである。

【００８９】

図示実施形態例に従って本発明を説明したが、本発明はこれに限定されるものではない。例えば、実施形態例では、図２に示すようなテーブル構造を持つブルートフォース用文字テーブル１５を想定したが、本発明は、このようなテーブル構造を持つブルートフォース用文字テーブル１５にその適用が限定されものではない。

【００９０】

【発明の効果】

以上説明したように、本発明によれば、パスワードに含まれる文字列について、その強度が出力されることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【００９１】

そして、本発明によれば、パスワードの持つ各文字毎に、その強度が出力されることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【００９２】

そして、本発明によれば、パスワードの持つ文字の文字強度の推移値が出力さ

れることになるので、ユーザは、パスワードのどの部分が強くどの部分が弱いのかを把握できるようになり、これにより、強いパスワードを作成することができるようになる。

【図面の簡単な説明】

【図１】

本発明を具備するパスワード作成支援装置の一実施形態例である。

【図２】

ブルートフォース用文字テーブルのテーブル構造の一例である。

【図３】

文字列強度算出プログラムの実行する処理フローである。

【図４】

パスワード強度検査画面の説明図である。

【図５】

パスワード強度検査画面の説明図である。

【図６】

文字強度算出プログラムの実行する処理フローである。

【図７】

パスワード強度検査画面の説明図である。

【図８】

文字強度推移値算出プログラムの実行する処理フローである。

【図９】

文字強度推移値算出プログラムの実行する処理フローである。

【図１０】

パスワード強度検査画面の説明図である。

【図１１】

文字強度推移値の変換処理の説明図である。

【図１２】

パスワード強度検査画面の説明図である。

【図１３】

パスワード強度検査画面の説明図である。

【図１４】

ブルートフォース攻撃の説明図である。

【符号の説明】

１　　パスワード作成支援装置

１０　入出力装置

１１　パスワード候補生成ルーチン

１２　文字列強度算出プログラム

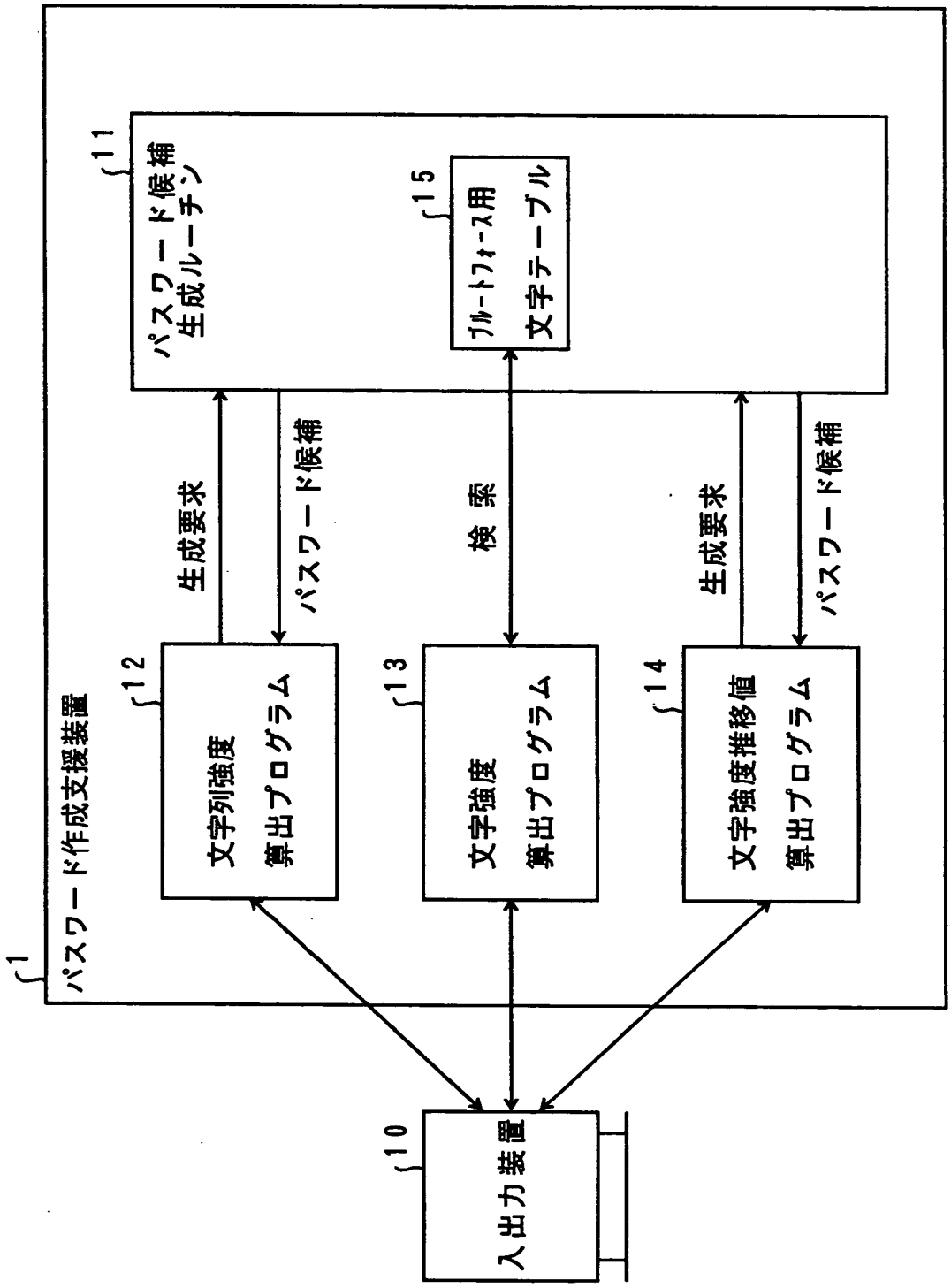
１３　文字強度算出プログラム

１４　文字強度推移値算出プログラム

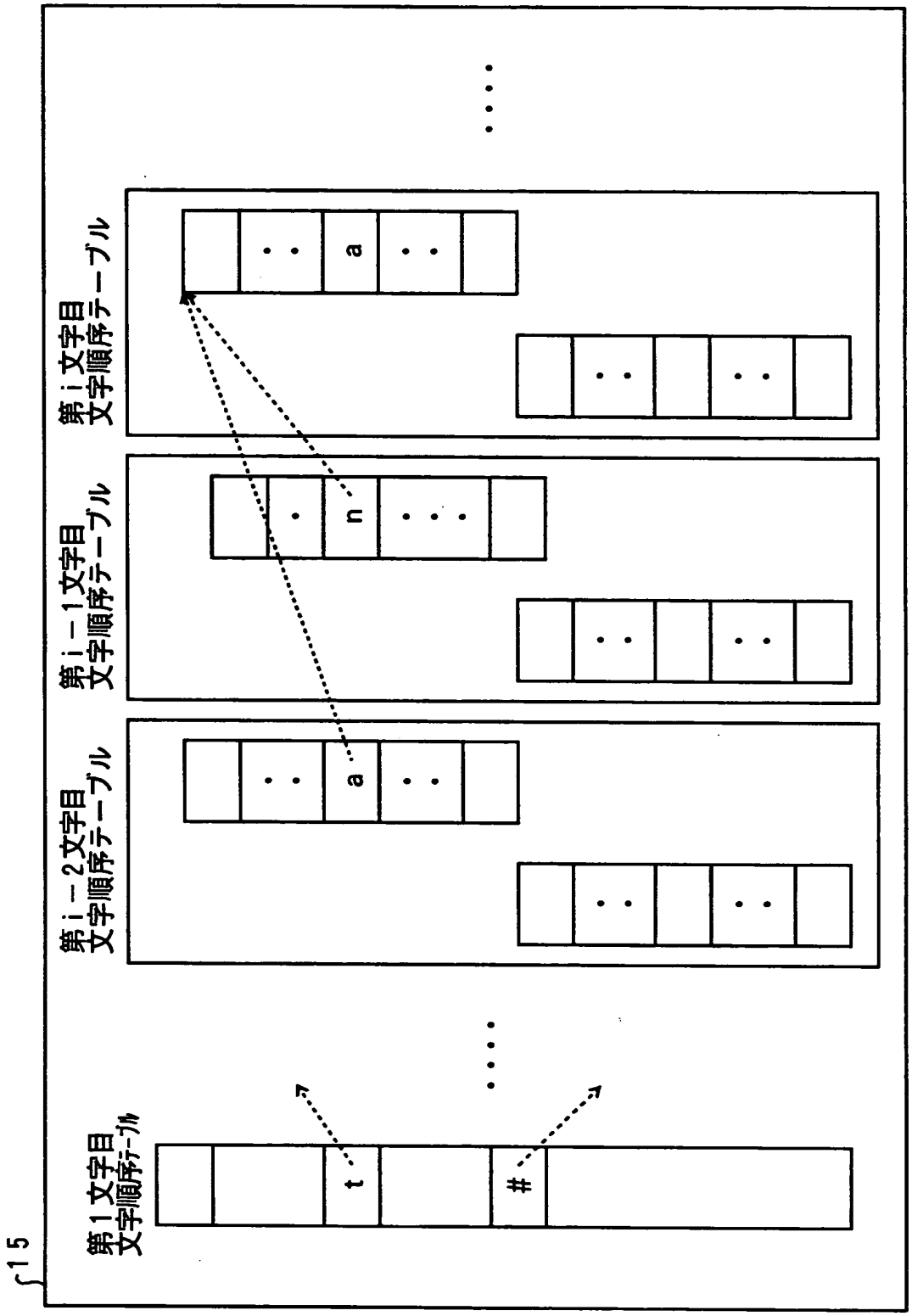
１５　ブルートフォース用文字テーブル

【書類名】　図面

【図１】

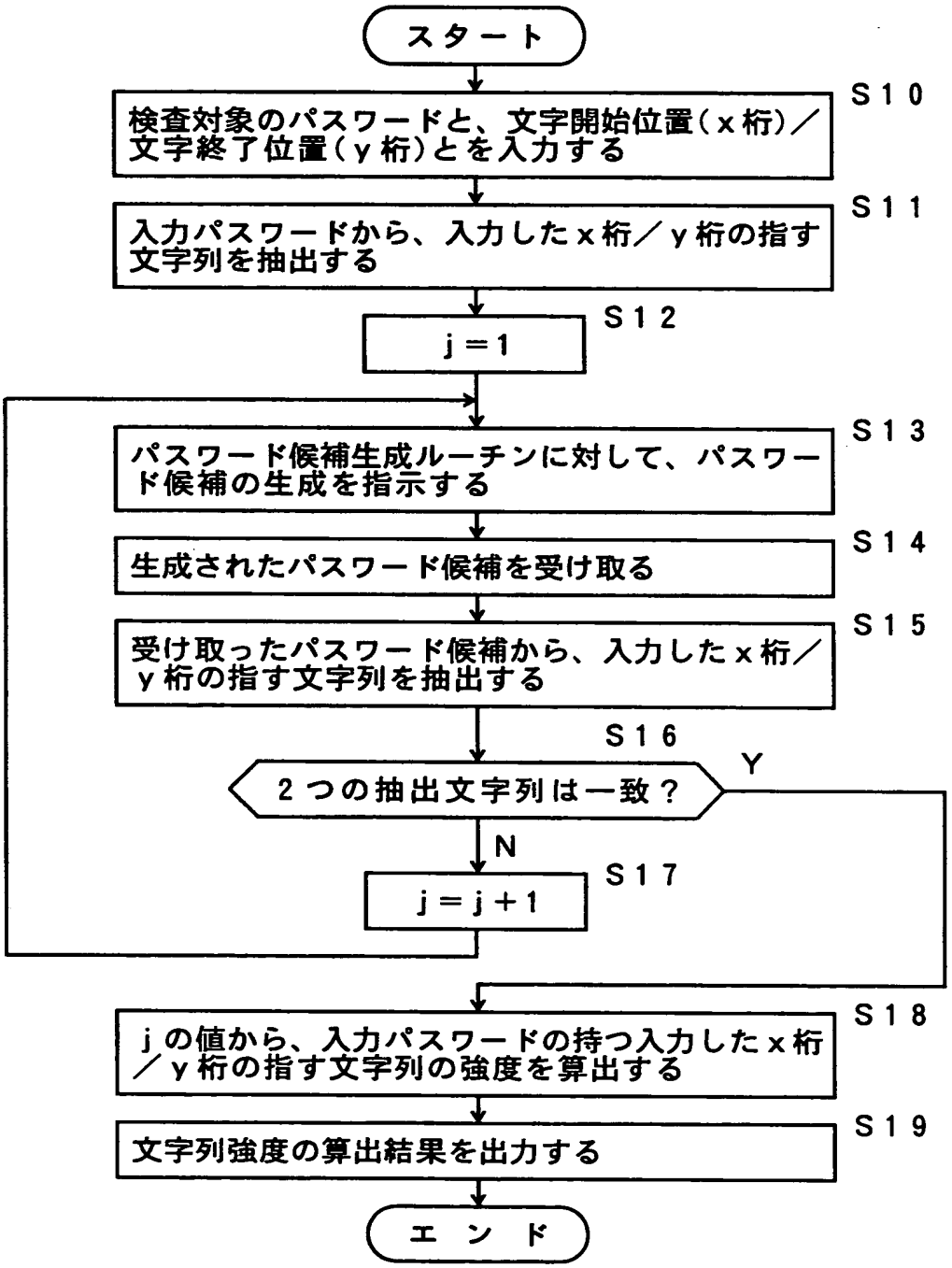

1
パスワード作成支援装置
11
パスワード候補
生成ルーチン
15
ブルートフォース用
文字テーブル
生成要求
パスワード候補
検索
生成要求
パスワード候補
12
文字列強度
算出プログラム
13
文字強度
算出プログラム
14
文字強度推移値
算出プログラム
10
入出力装置

【図２】

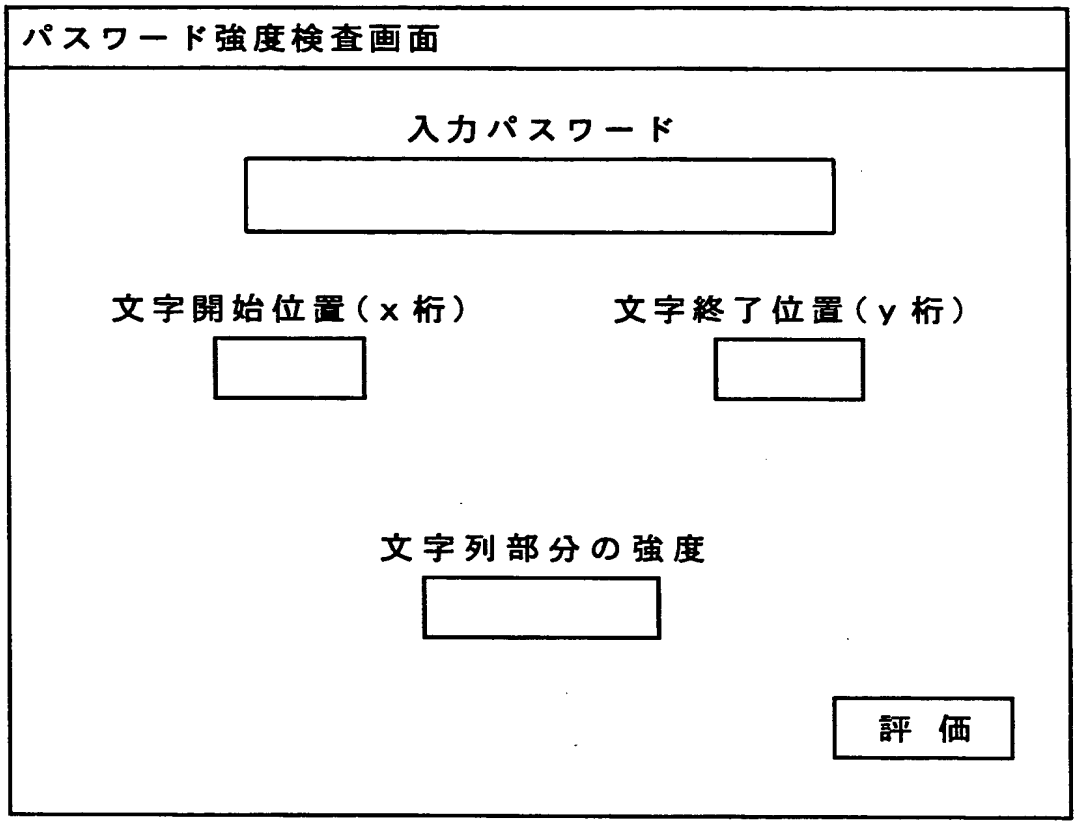


出証特２００３－３０５３４６７

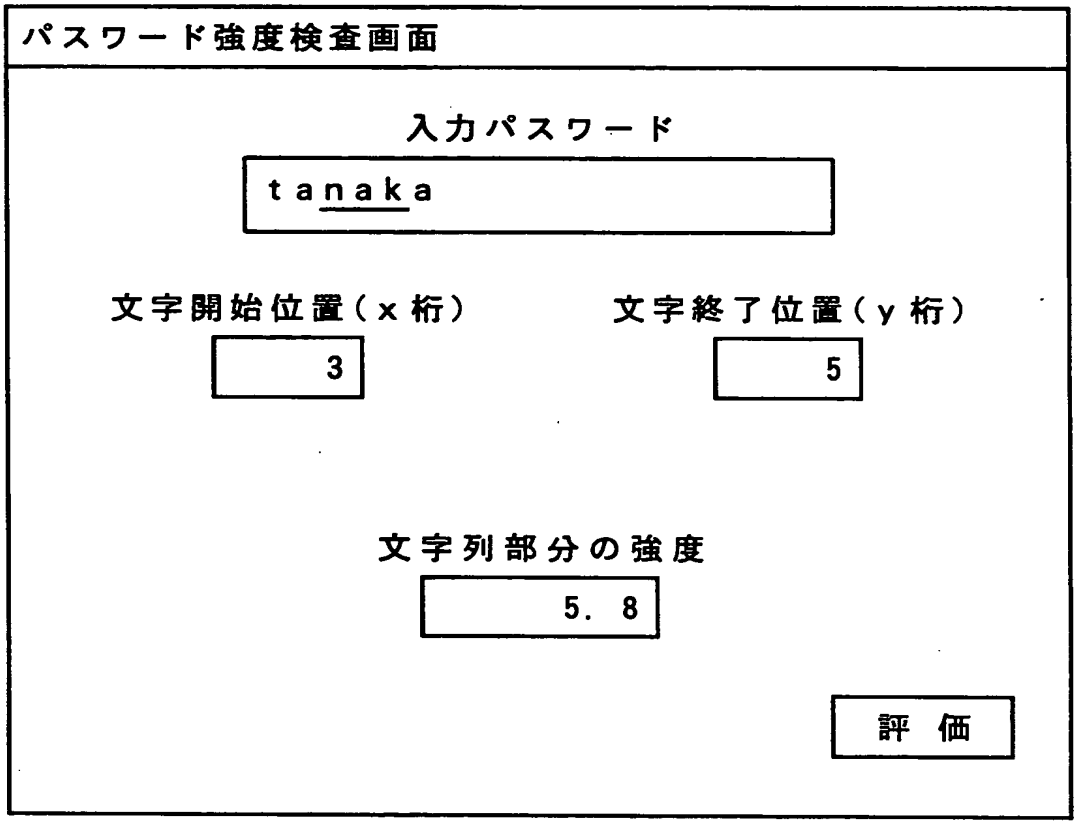
【図３】


スタート
検査対象のパスワードと、文字開始位置（ｘ桁）／文字終了位置（ｙ桁）とを入力する
Ｓ１０
入力パスワードから、入力したｘ桁／ｙ桁の指す文字列を抽出する
Ｓ１１
ｊ＝１
Ｓ１２
パスワード候補生成ルーチンに対して、パスワード候補の生成を指示する
Ｓ１３
生成されたパスワード候補を受け取る
Ｓ１４
受け取ったパスワード候補から、入力したｘ桁／ｙ桁の指す文字列を抽出する
Ｓ１５
Ｓ１６
２つの抽出文字列は一致？
Ｙ
Ｎ
ｊ＝ｊ＋１
Ｓ１７
ｊの値から、入力パスワードの持つ入力したｘ桁／ｙ桁の指す文字列の強度を算出する
Ｓ１８
文字列強度の算出結果を出力する
Ｓ１９
エ　ン　ド

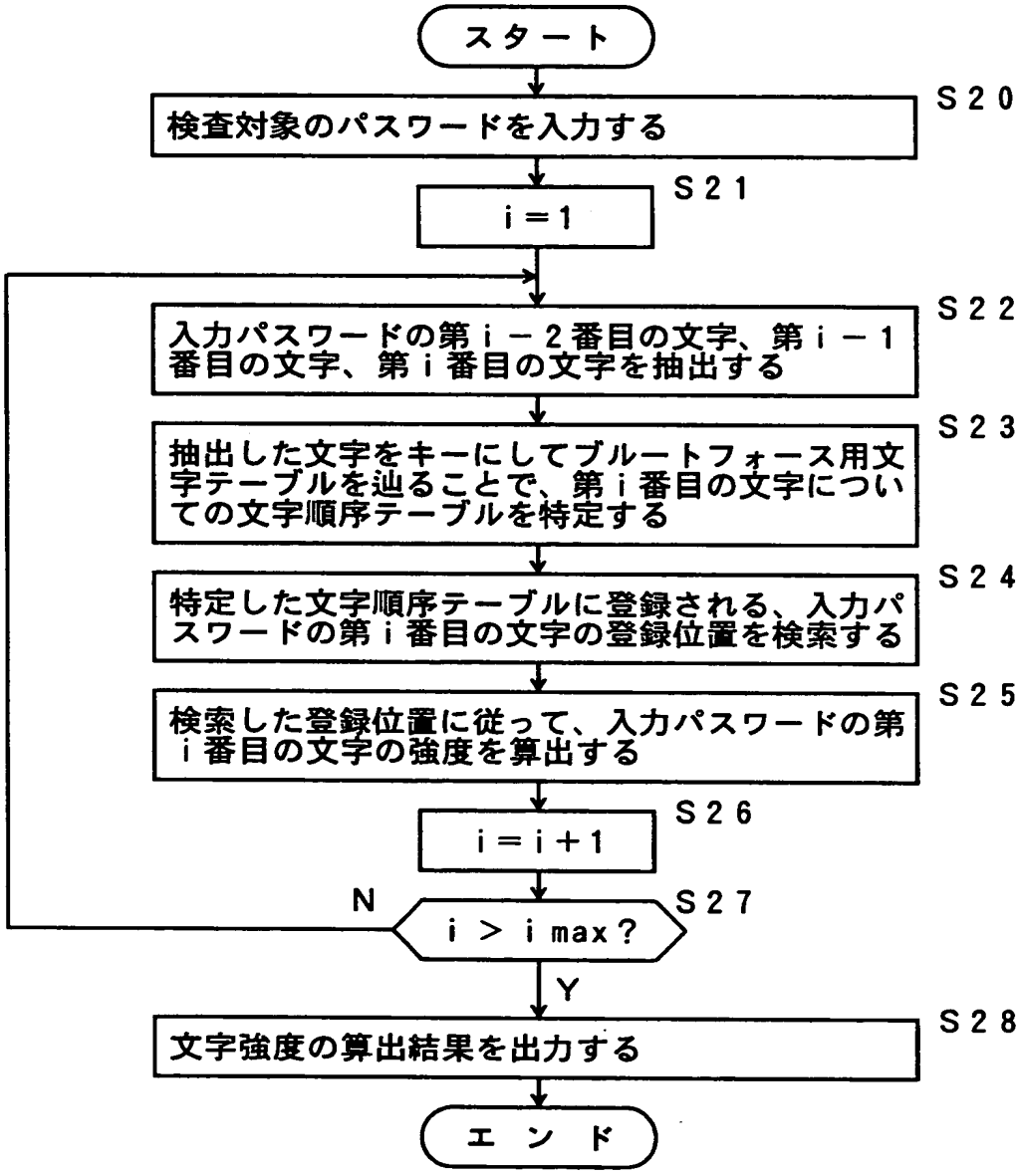
【図４】



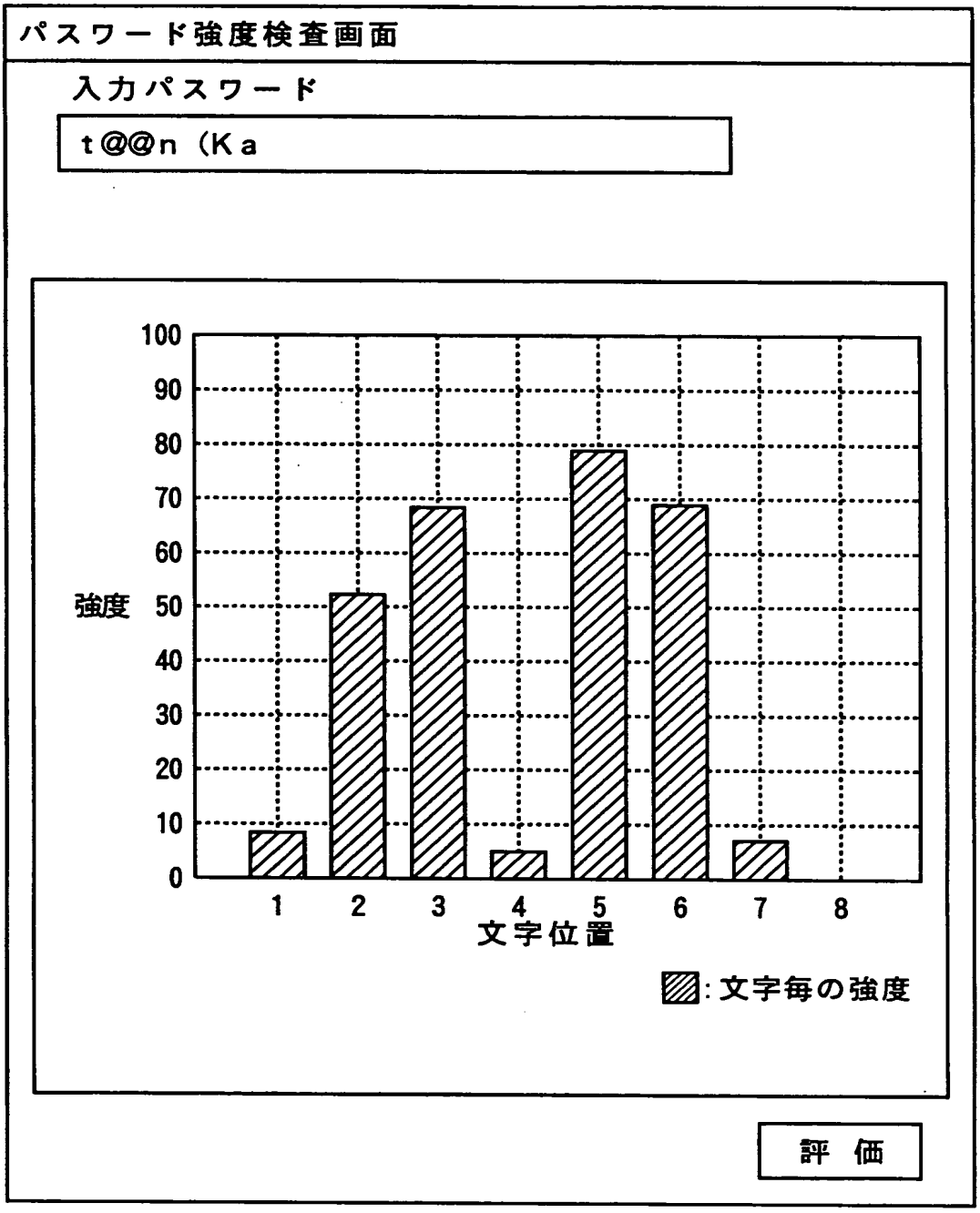
【図５】


パスワード強度検査画面
入力パスワード
tanaka
文字開始位置（x 桁）
3
文字終了位置（y 桁）
5
文字列部分の強度
5．8
評 価

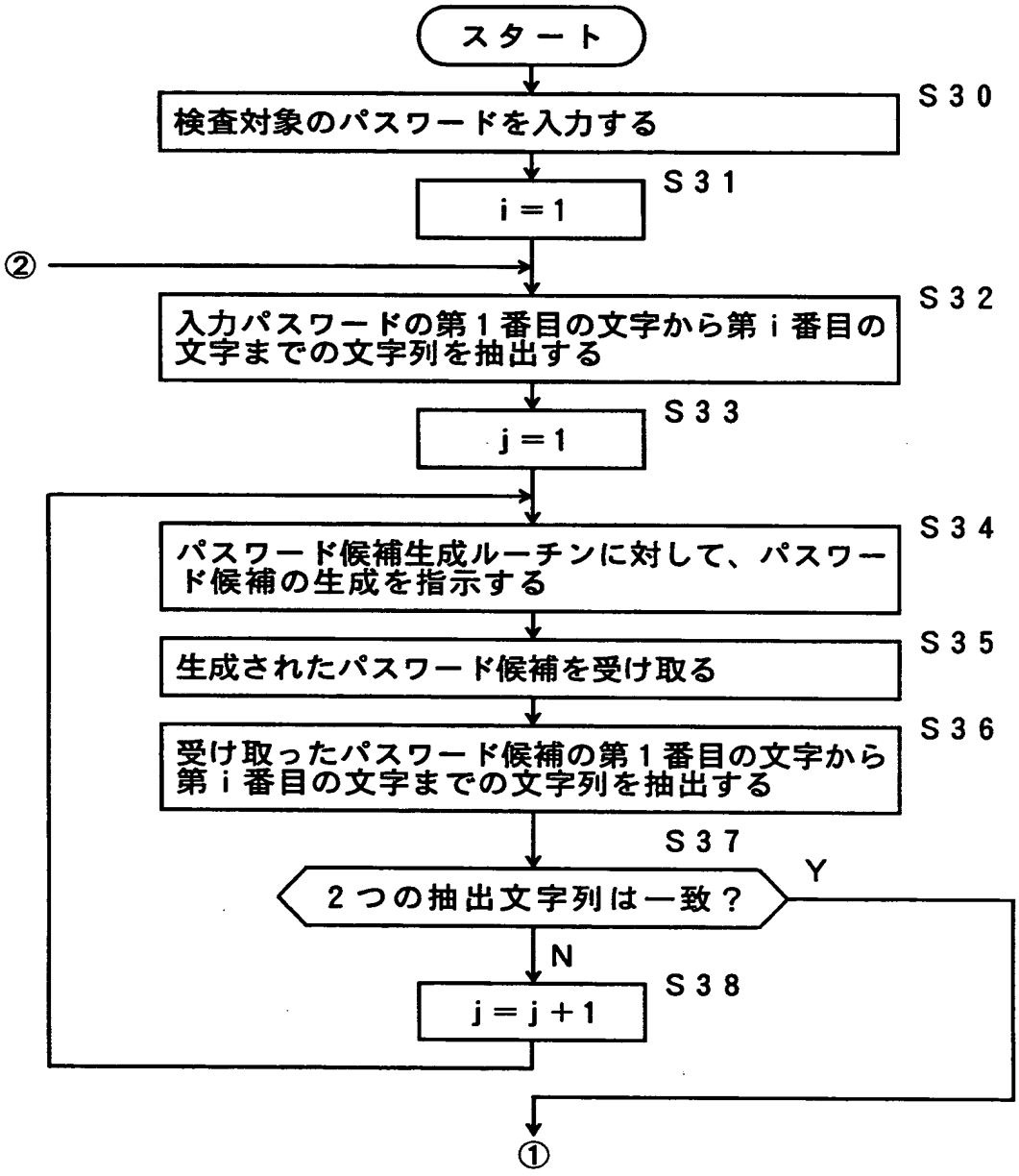
【図６】


スタート
検査対象のパスワードを入力する
S２０
i＝1
S２１
入力パスワードの第ｉ－２番目の文字、第ｉ－１番目の文字、第ｉ番目の文字を抽出する
S２２
抽出した文字をキーにしてブルートフォース用文字テーブルを辿ることで、第ｉ番目の文字についての文字順序テーブルを特定する
S２３
特定した文字順序テーブルに登録される、入力パスワードの第ｉ番目の文字の登録位置を検索する
S２４
検索した登録位置に従って、入力パスワードの第ｉ番目の文字の強度を算出する
S２５
i＝i＋1
S２６
N
i ＞ i max？
S２７
Y
文字強度の算出結果を出力する
S２８
エ ン ド

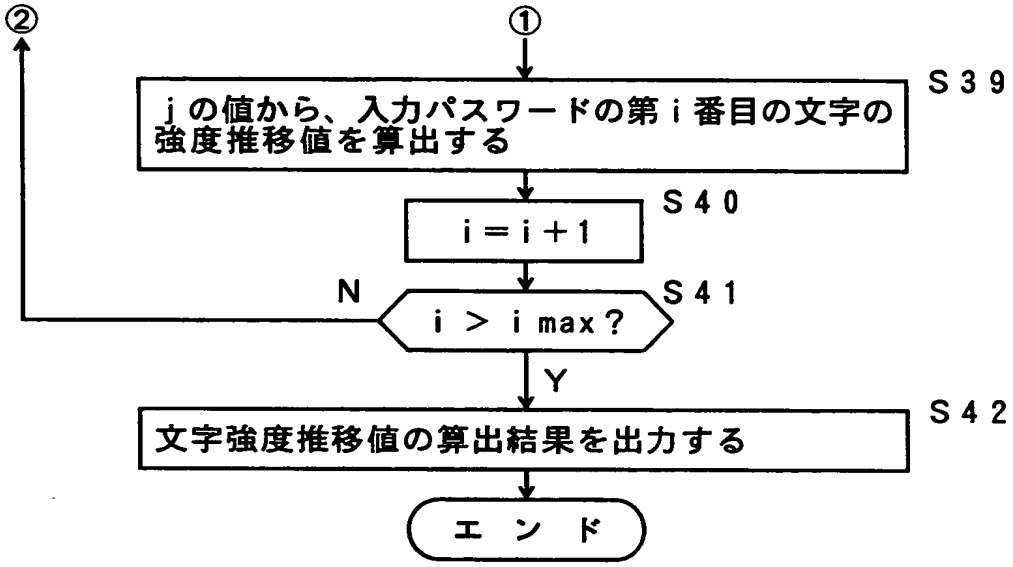
【図７】


パスワード強度検査画面
入力パスワード
t@@n（Ka
100
90
80
70
60
50
40
30
20
10
0
強度
1
2
3
4
5
6
7
8
文字位置
：文字毎の強度
評 価

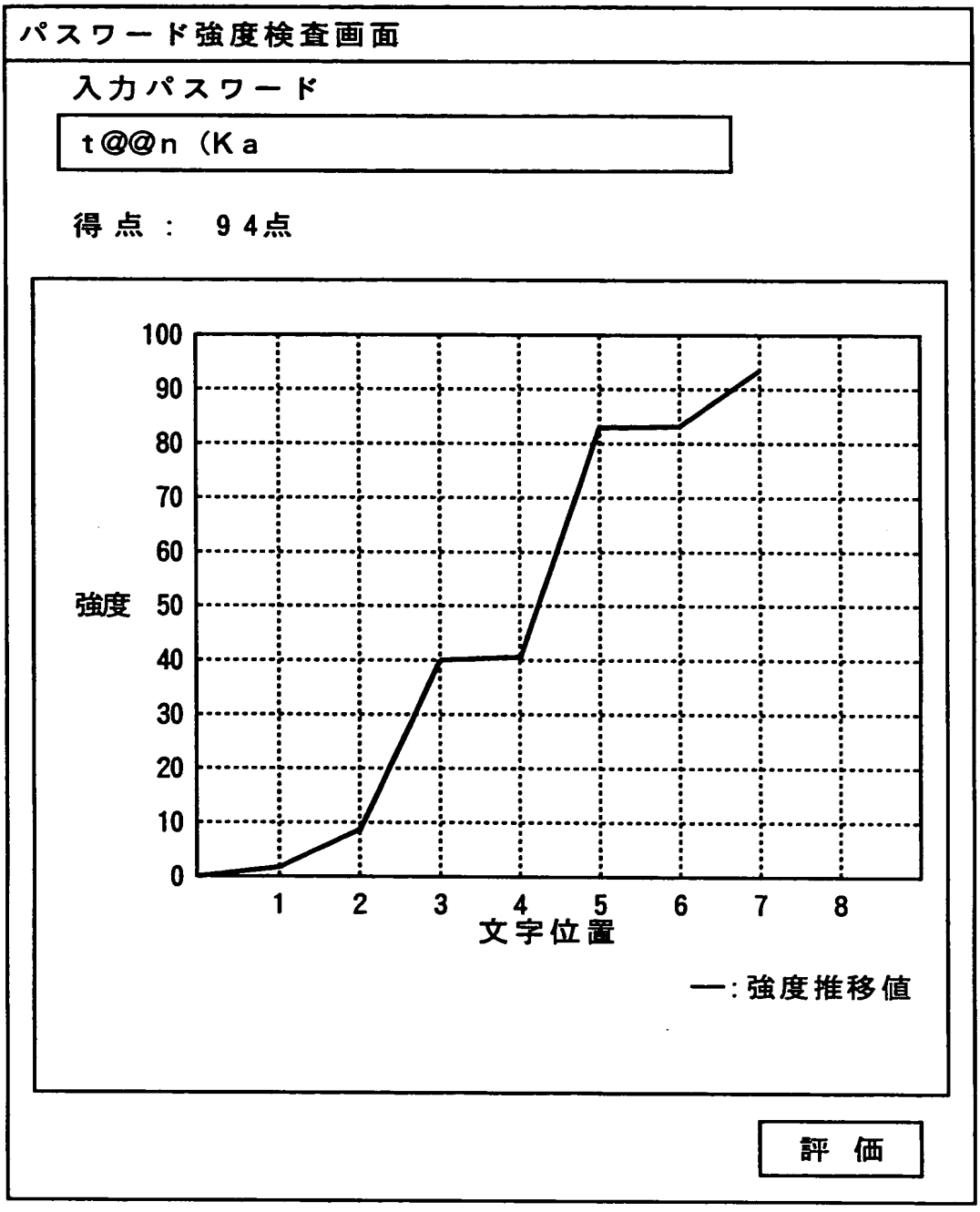
【図８】


スタート
検査対象のパスワードを入力する
S３０
i＝1
S３１
②
入力パスワードの第１番目の文字から第ｉ番目の文字までの文字列を抽出する
S３２
j＝1
S３３
パスワード候補生成ルーチンに対して、パスワード候補の生成を指示する
S３４
生成されたパスワード候補を受け取る
S３５
受け取ったパスワード候補の第１番目の文字から第ｉ番目の文字までの文字列を抽出する
S３６
S３７
２つの抽出文字列は一致？
Y
N
j＝j＋1
S３８
①

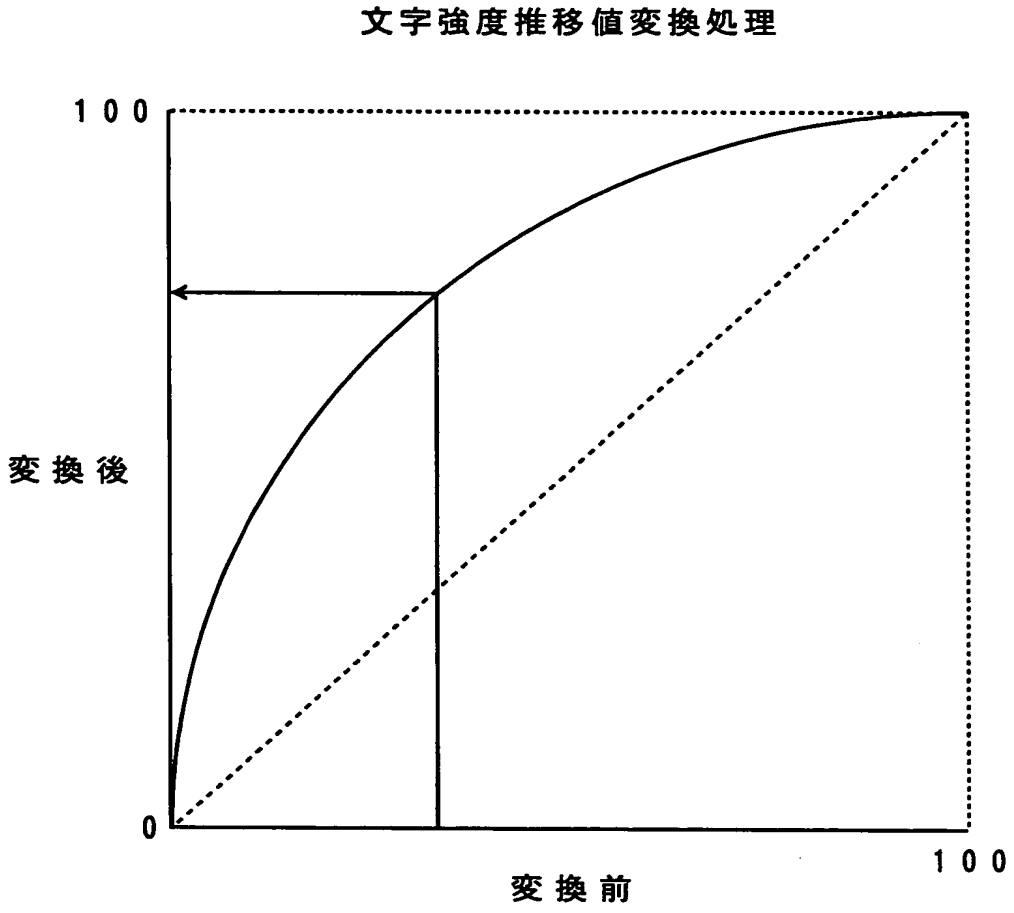
【図９】


①
ｊの値から、入力パスワードの第ｉ番目の文字の強度推移値を算出する
S39
ｉ＝ｉ＋１
S40
N
ｉ ＞ ｉ max？
S41
Y
文字強度推移値の算出結果を出力する
S42
エ ン ド
②

【図１０】

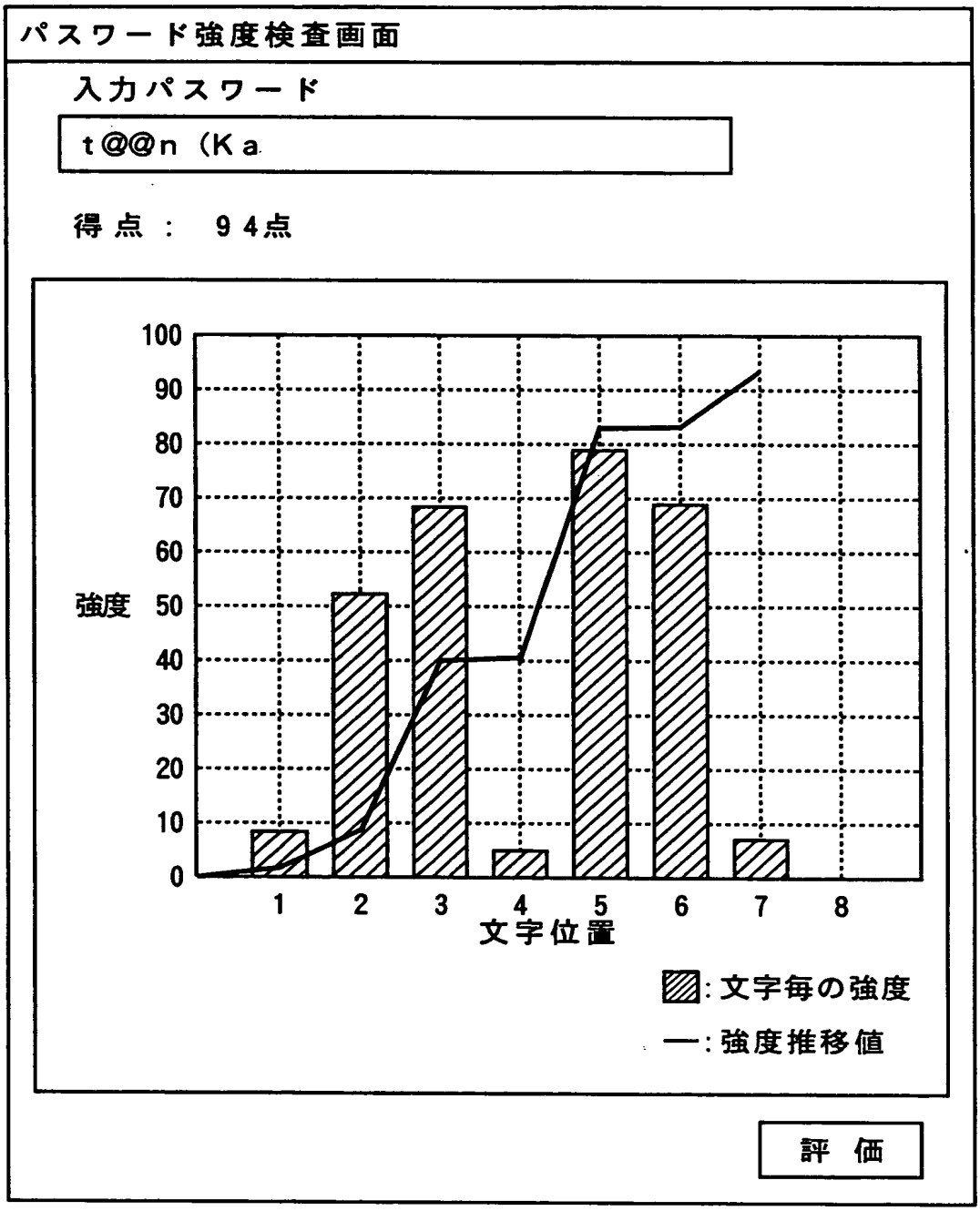

パスワード強度検査画面
入力パスワード
t@@n（Ka
得点：　９４点
100
90
80
70
60
50
40
30
20
10
0
強度
1
2
3
4
5
6
7
8
文字位置
—:強度推移値
評　価

【図１１】

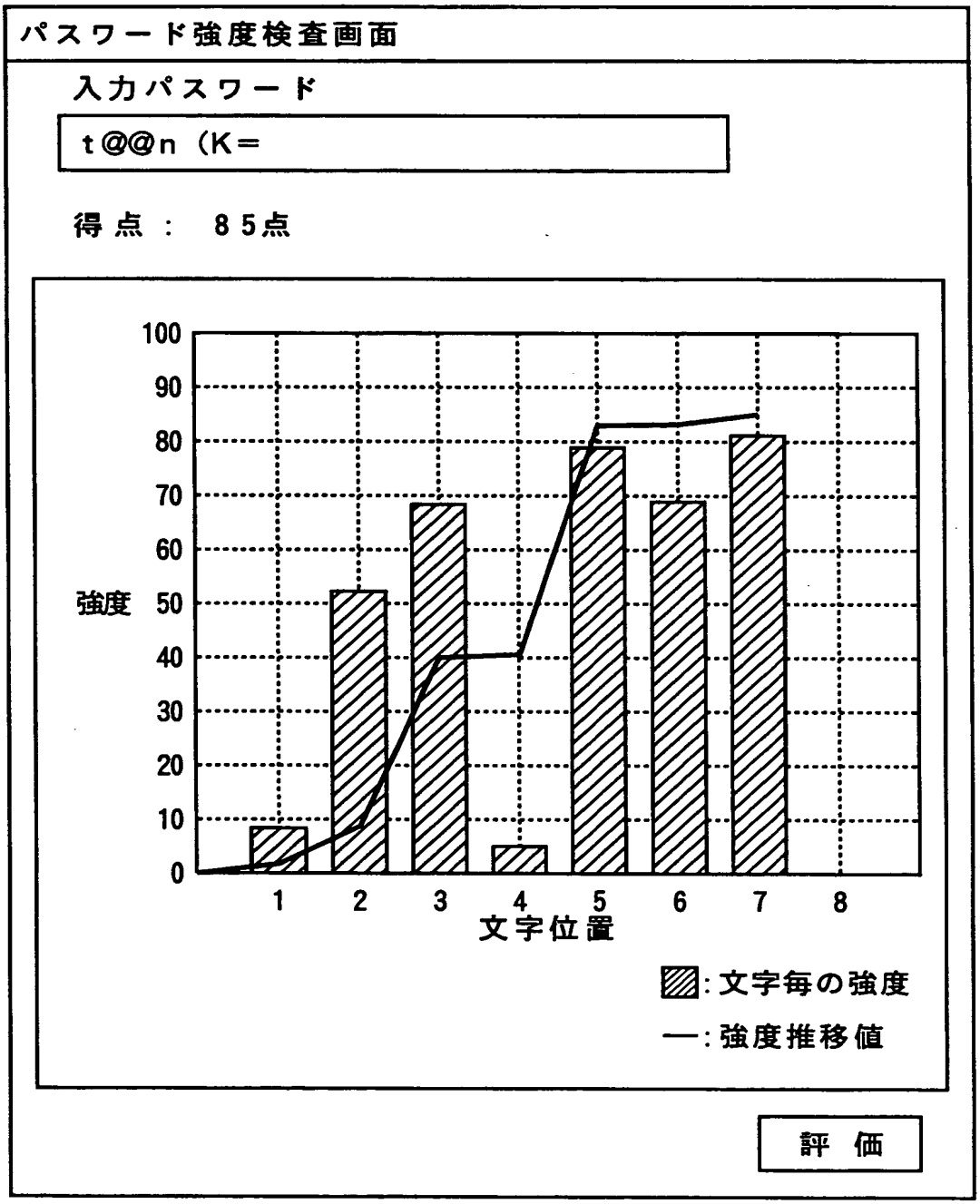


出証特２００３－３０５３４６７

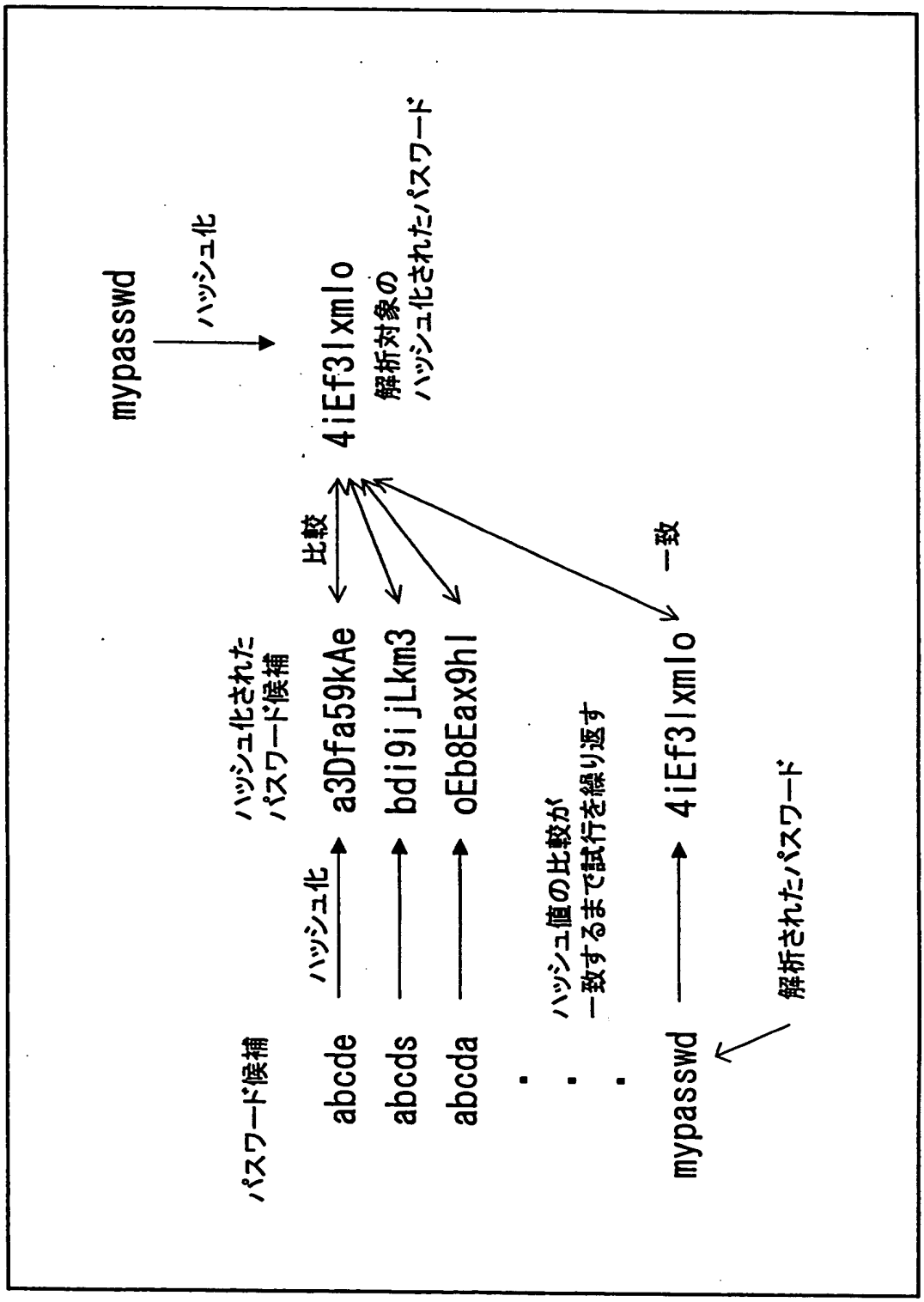
【図１２】


パスワード強度検査画面
入力パスワード
t@@n（Ka
得点：　９４点
100
90
80
70
60
50
40
30
20
10
0
強度
1
2
3
4
5
6
7
8
文字位置
：文字毎の強度
：強度推移値
評　価

【図１３】


パスワード強度検査画面
入力パスワード
t@@n（K＝
得点：　８５点
100
90
80
70
60
50
40
30
20
10
0
強度
1
2
3
4
5
6
7
8
文字位置
：文字毎の強度
：強度推移値
評　価

【図１４】


mypasswd
ハッシュ化
4iEf3lxmlo
解析対象の
ハッシュ化されたパスワード
比較
一致
ハッシュ化された
パスワード候補
パスワード候補
ハッシュ化
abcde
a3Dfa59kAe
abcds
bdi9ijLkm3
abcda
oEb8Eax9hl
ハッシュ値の比較が
一致するまで試行を繰り返す
mypasswd
4iEf3lxmlo
解析されたパスワード

【書類名】　　要約書

【要約】

【課題】本発明は、パスワードのどの部分が強くどの部分が弱いのかを分析して出力する新たなパスワード作成支援技術の提供を目的とする。

【解決手段】パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成するパスワード候補生成ツールを使って、検査対象の文字列を持つパスワード候補が最初に生成されるまでの生成個数を取得して、それに従って検査対象の文字列の強度を算出する。また、パスワードの各文字がブルートフォース攻撃に用いられるテーブルのどの位置に登録されているのか情報を取得して、それに従ってパスワードの各文字の強度を算出する。また、パスワードの先頭の文字を開始文字として、１文字ずつ長さの長くなる文字列を抽出して、それらの文字列を持つパスワード候補が最初に生成されるまでの生成個数を取得して、それに従ってパスワードの文字強度の推移値を算出する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６６６６〕

１．変更年月日　　１９９８年　７月　１日
［変更理由］　名称変更
住　所　東京都渋谷区渋谷２丁目１２番１９号
氏　名　株式会社山武